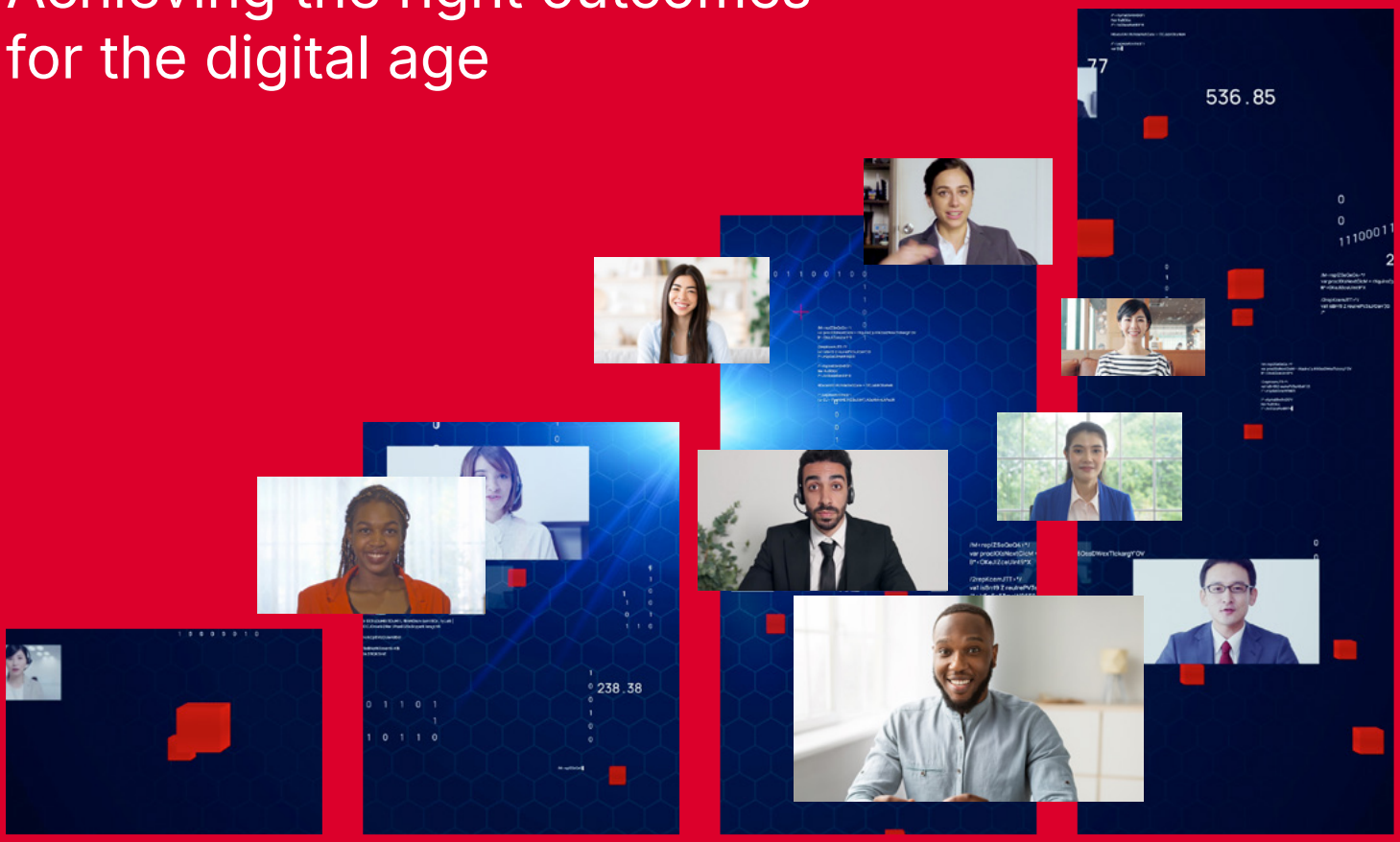
GSMA

Smart Implementation of Data Privacy Laws

Achieving the right outcomes for the digital age



GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at **gsma.com**

Contents

Introduction

Supervisory authorities face numerous challenges in implementing data privacy laws, whether they are an emerging authority implementing a new law or a well-established authority having to consider how to modify the implementation of an existing law.

The nascent authority may, for example, have significant staffing or budgetary constraints or additional mandates to implement telecommunications and/or financial laws. The well-established authority may have to simplify or improve its current data privacy law implementation due to the interplay with different sectoral laws, regulations or technological developments. It may need to consider how to simplify the current implementation of the national data privacy law.

How implementation is handled by a supervisory authority will impact the digital economy and mobile ecosystem. If the approach is overly strict and prescriptive or, conversely, lacking clarity or with contradictory and overlapping requirements, the regulatory complexity for organisations such as mobile network operators (MNOs) can increase compliance costs while failing to protect consumers as intended.

In the GSMA's 2019 Smart Data Privacy Laws report[1], 14 guiding principles were outlined, aimed at helping governments, policymakers and organisations to develop effective, future-proof data privacy frameworks.

This report builds on the 2019 report by providing insight into the implementation of each relevant principle, compiling learnings and good practice from around the world to assist those looking to implement data privacy laws in their market.

The key nine principles to consider when implementing a data privacy law are highlighted in Table 1 opposite. These are the principles associated most directly with the implementation decisions that authorities are typically faced with, and which help achieve the right outcomes for the digital age.

The following section considers the practical application of each of these principles, as countries adapt to a new or updated data privacy framework. While there is no single best approach, we strive here to provide recommendations drawn from real experience and reflecting input received through our engagement with data protection authorities and MNOs worldwide. All quotes stem from GSMA engagement with data protection authorities, regulators and industry stakeholders at the GSMA Ministerial Programme at MWC Barcelona, GSMA Capacity Building and regional events, the Global Privacy Assembly and the African Network of Data Protection Authorities annual conference.

1 https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2019/06/GSMA_Smart-Data-Privacy-Laws_Report_June-2019.pdf.

TABLE 1

A smart data privacy law is one that:

1	Takes the national law, traditions and culture as its starting point.
2	**Finds alignment with existing international norms and data privacy frameworks.**
3	**Is underpinned by the concept of accountability.**
4	Is based on flexible principles rather than excessively prescriptive requirements.
5	**Is based on preventing or limiting the risk of harm.**
6	**Applies horizontally without reference to a specific sector or technology.**
7	Achieves the right balance between ex ante and ex post.
8	Has a definition of personal data that is in line with international definitions.
9	**Provides a range of flexible lawful grounds for processing, not just consent.**
10	**Includes a range of rights to empower individuals.**
11	**Has a pragmatic approach to data breach notifications.**
12	**Promotes cross-border data flows.**
13	Establishes an independent supervisory authority for data privacy.
14	**Provides a range of remedies, enforcement measures and sanctions that are proportionate to the harm and take an organisation's good practices into account.**

Source: https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2019/06/GSMA_Smart-Data-Privacy-Laws_Report_June-2019.pdf

Implementing guiding principles of smart data privacy law

International norms and frameworks

PRINCIPLE | A smart data privacy law is one that finds alignment with existing international norms and data privacy frameworks.

A data privacy framework is a comprehensive set of guidelines, regulations, principles and practices designed to safeguard personal data and uphold individuals' rights. This includes national or regional laws[2] and international instruments[3], as well as tools, standards and best-practice frameworks implemented by organisations[4].

Implementing a data privacy framework varies from one country to another, but a key step involves defining and clarifying the framework according to the legal and institutional context and local circumstances.[5] This includes the following:

- Crafting a narrative that explains:
  a. Who the main stakeholders are, including if any sector-specific supervisory authorities are engaged.
  b. Who is required to comply with the data privacy framework.
  c. The components of the framework and their applicability in practice.
  d. Why the adopted framework matters and its intended impact.
- Assessing whether specific examples and use cases are required to aid understanding.

2 For example, the E.U General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Brazil General Data Protection Law (LGPD), and the Singapore Personal Data Protection Act (PDPA).
3 For example, EU-US Data Privacy Framework; Asia-Pacific Economic Cooperation (APEC) Privacy Framework.
4 For example, National Institute of Standards and Technology (NIST) Privacy Framework; International Organization for Standardization (ISO) 27701 Standard.
5 Data Governance Toolkit: https://www.broadbandcommission.org/wp-content/uploads/2025/07/Data-Governance-Toolkit.pdf.

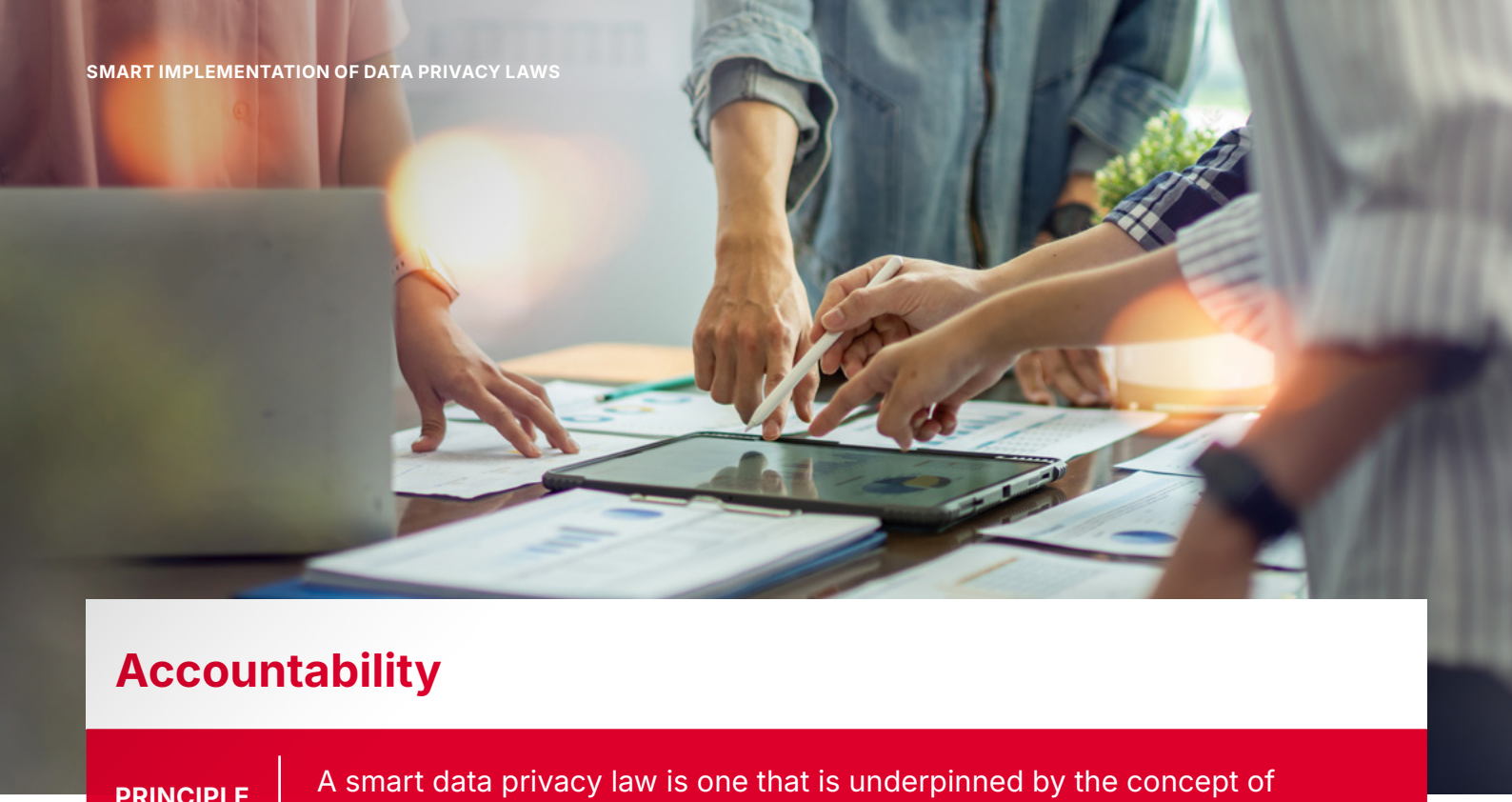
"Resource constraints, budget constraints, the interplay with other policy and regulatory frameworks and awareness are the main limitations to implementing cost-effective, efficient and sustainable data privacy frameworks."

Stakeholders' observation at the 46th Global Privacy Assembly, Jersey 2024; MWC Future-Proofing Data Privacy Roundtable with Data Protection Authorities, and Capacity Building NADPA-RAPDP Conference and AGM, Abuja 2025.

To achieve a successful and smart implementation outcome, it is important that the supervisory authority take responsibility to evangelise the new law and explain its impact on, and benefits for, consumers, businesses and organisations across the digital economy. Throughout this process, it is essential to be clear, proactive and consultative:

- Informing individuals and stakeholders of the purpose of the framework, what it comprises, what the authority intends to do with the framework and how it will implement it.
- Making individuals and stakeholders aware of how the framework works, with specific, relatable examples.
- Giving individuals and stakeholders straightforward explanations on why the framework matters, and engaging with them to hear their views, at initial stages and to evaluate outcomes and consider future improvements.

Smart Implementation	Examples
Provide clarity An ideal framework should provide the 'what, why, when, who and how' rationale. Individuals must be made aware of the framework, its context, and how it will be implemented, with specific examples.	**Evaluate** whether the data privacy laws and frameworks are practical and relevant by considering the country's digital economy strategy and align the framework with any other sector-specific supervisory authorities' mandates. **Be technology-neutral** and creative when explaining and promoting the framework, avoiding complicated legal terminology, language and tone. **Provide examples** for how the risk-based approach applies and provide examples of scenarios that would require consultation with industry. **Assess** whether the data privacy framework is aligned with other international data privacy frameworks. If so, identify the relevant parts of the framework that align, dissect the commonalities and consider unified interoperability.



Accountability

PRINCIPLE | A smart data privacy law is one that is underpinned by the concept of accountability.

A smart data privacy law incentivises or requires accountability mechanisms, drawing on good practice that exists in local and global legal instruments.

When the accountability principle is implemented effectively, organisations not only seek to comply but are also able to demonstrate how they comply. Supervisory authorities then take an organisation's good data governance practices into consideration for administrative procedures or when deciding on enforcement action. This encourages effective compliance and promotes a high level of privacy protection.

In the mobile context, the GSMA has provided a range of guidance to MNOs through its GSMA Mobile Privacy Principles,[6] GSMA Privacy Design Guidelines for Mobile Application Development,[7] GSMA IoT Security Guidelines[8] and GSMA Mobile Money Certification[9].

These approaches can be recognised and encouraged by supervisory authorities as well as used by MNOs to demonstrate to consumers and supervisory authorities how they implement effective safeguards.

Implementation of the accountability principle can be facilitated by supervisory authorities by:

- Referencing and reviewing accountability incentives and other clear legislative frameworks adopted by other countries and regions and determining approaches that would work well in their market.
- Avoiding overly prescriptive requirements and, instead, encouraging mechanisms that reduce the administrative burden. For example:
  a. Codes of Conduct (COC), International Organisation for Standardisation (ISO) standards, certification and trust marks can be encouraged.
  b. In the context of cross-border data, existing mechanisms like Binding Corporate Rules (BCRs), Cross-Border Privacy Rules (CBPR) and Model Contractual Clauses (MCC) can be considered.

6 GSMA Mobile Privacy Principles: https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2012/03/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf.
7 GSMA Privacy Design Guidelines for Mobile Application: https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2018/02/GSMA-Privacy-Design-Guidelines-for-Mobile-Application-Development.pdf.
8 GSMA IoT Security Guidelines: https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2024/07/FS.60.pdf.
9 GSMA Mobile Money Certification: https://gsmamobilemoneycertification.com.

"Advancing accountability requires consensus between the mobile industry and supervisory authorities. It is crucial to demonstrate accountability as sector-agnostic and scalable, with tangible evidence and success stories."

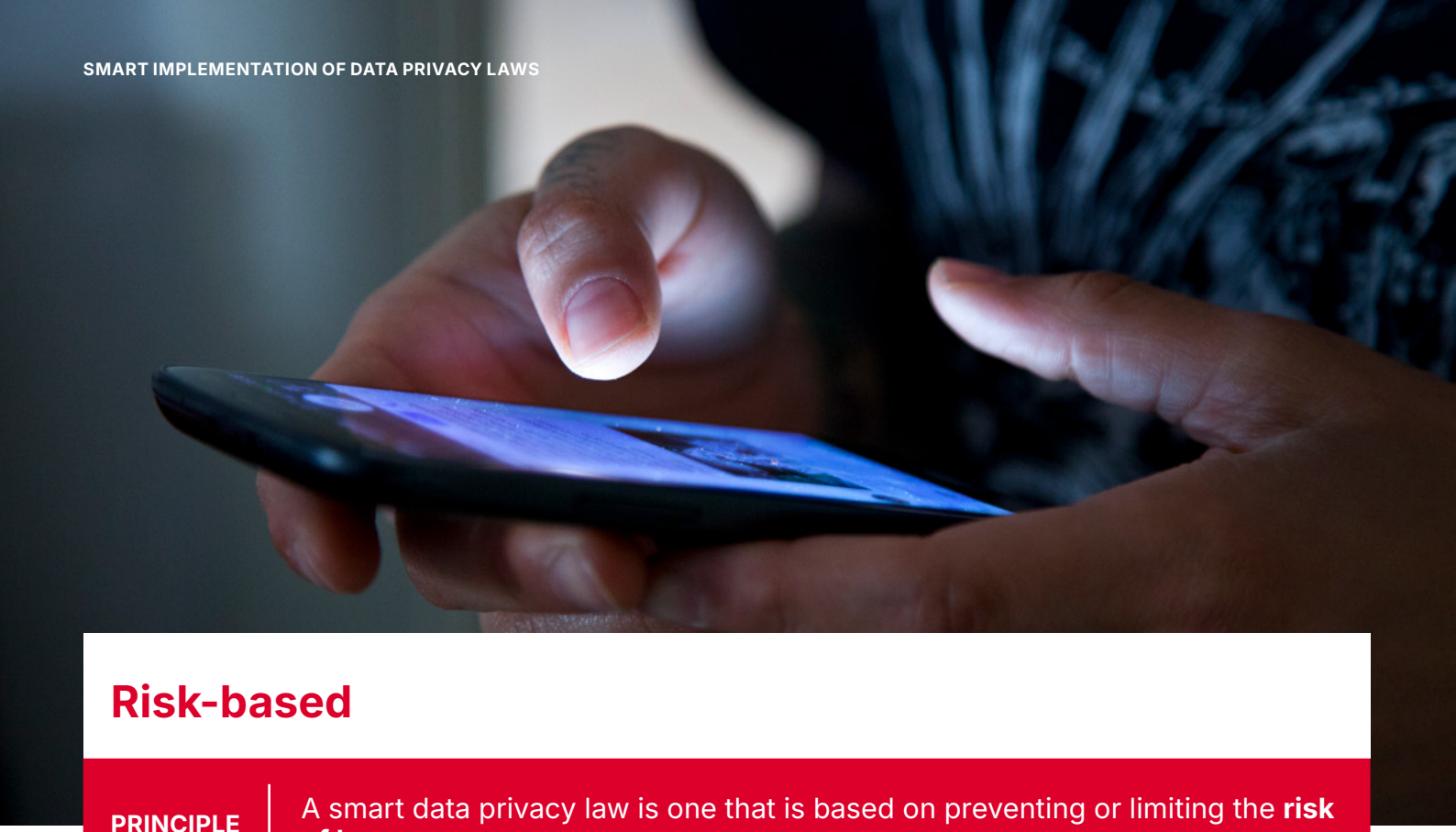
Stakeholders' consultation at the 46th Global Privacy Assembly, Jersey 2024 GSMA Roundtable: Smart Data Privacy Implementation in the Mobile Ecosystem.

For a successful and smart implementation outcome, it is important for the supervisory authority to embrace an accountability concept and put it at the heart of its implementation efforts. It is essential to:

- Apply a coordinated, consultative approach by:
  a. Working with other supervisory authorities at local, regional and global levels.
  b. Providing guidance to organisations on what good accountability and transparency looks like by way of pragmatic and relatable examples.
  c. Disseminating accountability guidelines to organisations through consistent outreach efforts.
- Understand the digital and mobile ecosystem and provide clear examples on how and when accountability should be demonstrated.[10]

Smart Implementation	Examples
Coordinate with other supervisory authorities **Provide guidance and consistent outreach to organisations**	**Global Privacy Sweep 2018:** Privacy Accountability by the Global Privacy Enforcement Network (GPEN). GPEN is an informal network of over 60 privacy enforcement authorities. In 2018, GPEN looked at how well organisations have implemented the core concepts of accountability into their own internal privacy policies and programmes.[11] **Asia Pacific Privacy Authorities (APPA) Privacy Awareness Week 2024:** the Personal Data Protection Bureau (PDPB) in Macao prepared a set of promotional posters and videos on the theme of "Privacy and technology: Improving transparency, accountability, and security.[12]

10 The AEPD approves Telefonica Group's Binding Corporate Rules: https://www.telefonica.com/en/communication-room/blog/aepd-approves-telefonica-groups-binding-corporate-rules/.
11 GPEN Sweep 2018: Privacy Accountability - https://ico.org.uk/media2/about-the-ico/documents/2614435/gpen-sweep-2018-international-report.pdf.
12 Improving accountability: https://www.appaforum.org/paw/resources/posters/.



Risk-based

PRINCIPLE | A smart data privacy law is one that is based on preventing or limiting the **risk of harm.**

A smart data privacy law includes provisions that target harm to individuals or thresholds for reporting data breaches. These are more effective as they encourage organisations to identify and mitigate risk. Application of the concepts of privacy-by-design, data privacy impact assessments (DPIA), privacy impact assessment (PIA) and transfer impact assessment (TIA) can all help evaluate, identify and mitigate organisations and individuals' risk impact throughout the lifecycle of a product, service or process.

In the mobile context, it is important to recognise that there are many parties involved in the application or service delivery chain that are responsible for collecting and processing a user's personal data for different purposes. These may include app developers, device manufacturers, online platforms, OS companies, mobile network operators, advertisers and analytics companies. It is important that all parties in the chain of delivery of any product or service play their part. The GSMA Privacy by Design Guidelines for Mobile Application Development recognise this and provide guidance intended to apply to all parties involved.

> "A risk-based approach does not change or replace any applicable legal requirements and does not alter the rights of individuals under data protection laws. It is an additional tool that improves data privacy compliance by linking privacy controls and mitigations to the likelihood and severity of the harms associated with processing personal data."
>
> Centre for Information Policy Leadership (CIPL) on the role of risk management in data protection.

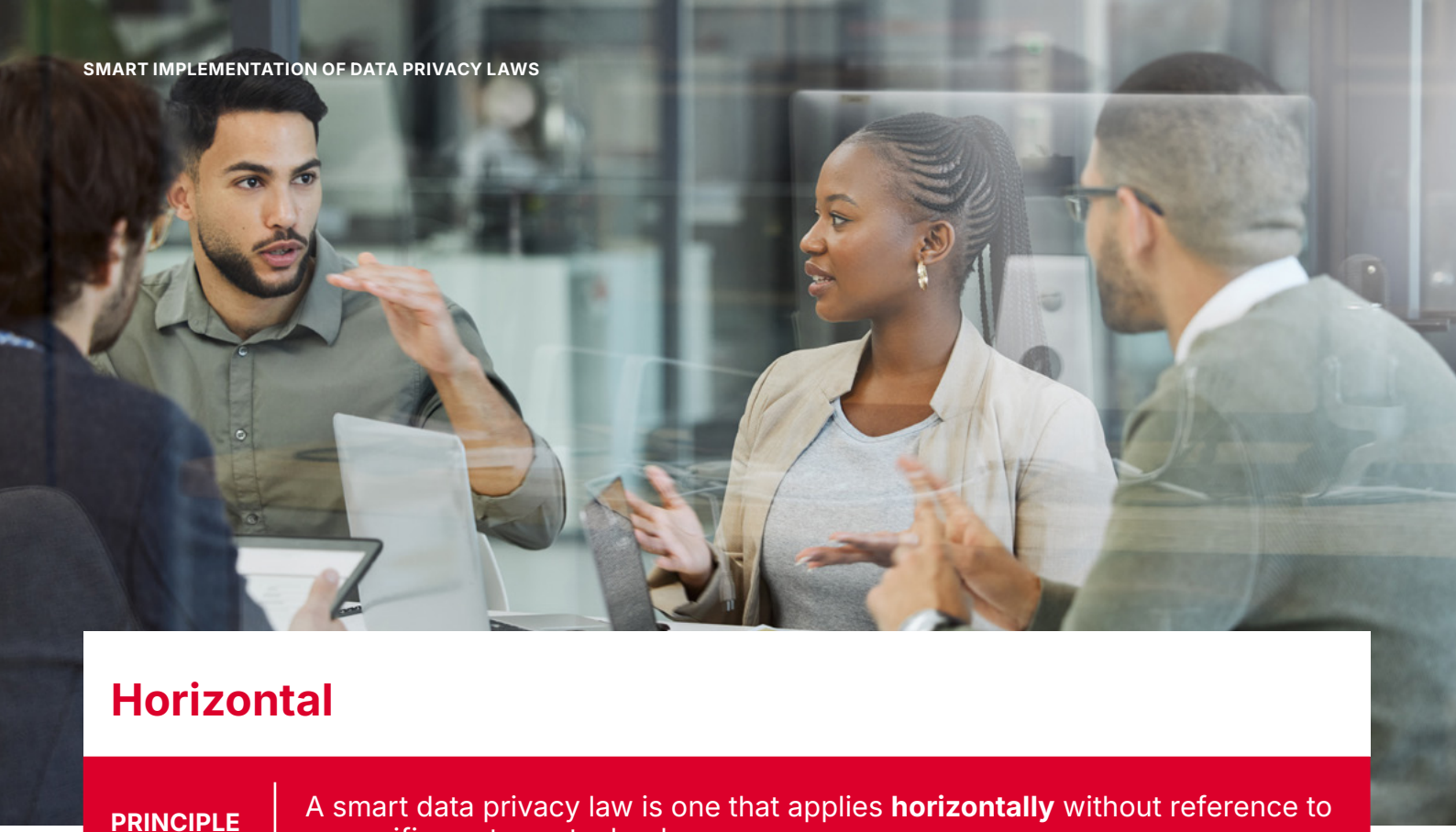
Implementing a risk-based approach means encouraging internal and external governance and processes which manage data privacy risk and help organisations carry out their own risk assessments. For example, DPIAs and PIAs are mechanisms used by organisations in a proactive manner to evaluate and minimise the impact of certain high-risk processing activities to individuals' privacy and fundamental rights. The benefits of the risk-based approach are far reaching. It enables organisations to demonstrate accountability, transparency, make thought through decisions and cultivate trust with their customers.

Crucially, it allows supervisory authorities to be strategic in how they prioritise enforcement action and manage their resources during consultation.

For a successful and smart implementation outcome, it is important that supervisory authorities:

- Define what a risk-based approach means and provide guidance on what is expected of organisations.
- Publish a strategy for enforcement for each term, so that individuals know what to expect and organisations know what they should prioritise as the most high-risk areas.

Smart Implementation	Examples
Define what a risk-based approach means and provide guidance	**Various supervisory authorities** have developed their own guidelines and toolkits on Data Privacy Impact Assessments to help organisations implement them effectively. They include: **France:** CNIL Guidelines on DPIA **New Zealand:** Office of the Privacy Commissioner, Te Mana Matapono Matatapu Privacy Impact Assessment Toolkit **Singapore:** Singapore Personal Data Protection Commission Guide to Data Protection Impact Assessments



Horizontal

PRINCIPLE | A smart data privacy law is one that applies **horizontally** without reference to a specific sector or technology.

A smart data privacy law will apply horizontally to the processing of personal data regardless of the sector or the technology used, providing a common baseline for all actors in the digital ecosystem and data-driven economy.

In the mobile context, the telecoms industry has long supported horizontal, sector-neutral and technology-neutral general data privacy laws. However, in some jurisdictions, supervisory authorities are mandated to enforce and implement sector-specific laws, such as telecom and financial services laws. This, along with redundant or overlapping rules in other laws, guidance or telecom licence conditions, often causes confusion and legal uncertainty for MNOs without providing additional protection for individuals and should therefore be reviewed and removed.

Implementing a data privacy law in a jurisdiction with sector-specific, overlapping or legacy rules can be challenging. It is crucially important to address any areas of confusion upfront:

Be precise: Tell individuals and organisations where confusion between the general data privacy law, telecommunications law and sectoral laws may arise – but don't overcomplicate with technical and or legal jargon or tone.

Be clear: Help individual and organisations to understand the reasons and the actionable steps to address confusion and misunderstanding.

Give examples: Make it clear and coherent by giving individuals and organisations relatable, easy-to-understand examples.

> "How do regulators tackle the challenge of overlapping policy domains? How do we handle the pushbacks from commercial organisations who play one regulator against another? Is there too much regulation, and is it compatible?"
>
> 46th Global Privacy Assembly, Jersey 2024, panel discussion.

For a successful and smart implementation outcome, it is crucial for the supervisory authority to:

- Break down requirements and provisions that are redundant or lead to broad, ambiguous and opaque interpretation.
- Ensure a clear hierarchy and cross-reference any sector-specific or overlapping laws to the general data privacy law requirements and provisions and integrate with the general data privacy laws.
- Work with other supervisory authorities on how to address present and future overlapping provisions and reporting requirements.
- Seek input from industry on operational issues and propose evidence-based harmonisation of rules.

Smart Implementation	Examples
Undertake legislative reforms	**Commence legislative reforms** to review and subsequently remove sector-specific laws, applying clear hierarchy and/or division of delegated authority and responsibility.
Seek input, identifying commonalities and applying a consistent approach	**Some countries / regions have sought input** through public consultation or directly from industry on operational issues, and proposed evidence-based harmonisation of rules: **Vietnam:** Vietnam's National Assembly passed the Law on Data. In March 2025, the Government issued public consultations on detailed regulations and implementation measures for the law on data, scientific, technological, and innovative activities and data-related services, national data development fund, and core and critical data classification. **European Union:** The European Commission sought input from MNOs into its Digital Networks Act (DNA) — a significant reform of the European Union's telecommunications regulations, helping the region to keep pace with the evolving digital landscape, where technological leadership is a critical geopolitical priority. www.digital-networks-act.com

Consent and lawful grounds for processing

PRINCIPLE | A smart data privacy law is one that provides a range of **flexible lawful grounds for processing**, not just consent.

Consent is not appropriate for all processing activities, and a smart data privacy law provides a range of lawful grounds for processing personal data. Common grounds include compliance with legal obligations, performance of a contract, to protect vital interests of the individuals, for legitimate interests of the data controller which requires the organisation to balance competing interests and risks.

In the mobile context, users often experience 'consent fatigue' and in other cases, for example when scammers take control of an individual's account, consent is not the appropriate basis for processing data. To avoid these scenarios, it is important that organisations have flexible and dynamic means to manage and refresh consent through their systems preferences or dashboards. For example, some MNOs integrate their consent management platform with legitimate interest assessment platforms or other lawful grounds of processing.

> "Consent is not a silver bullet for data privacy compliance."
>
> Elizabeth Denham CBE, Information Commissioner 2016-2021.

For a successful and smart implementation outcome it is important that supervisory authorities:

- Educate on which legal basis is appropriate and how to carefully evaluate the most appropriate lawful basis of processing that reflects the true nature of the relationship between the organisation and the individual, and the purpose of the processing.
- Adopt easy-to-understand and less prescriptive terms when drafting and disseminating consent and other lawful grounds of processing.
- Be pragmatic when providing illustrations on consent and other lawful grounds of processing. For example:
  - The UK ICO provides advice aimed at private sector organisations across the digital economy that want to share personal information with each other to support scam and fraud mitigation efforts.

Smart Implementation	Examples
Educate on which legal basis is appropriate and in which context	**Many supervisory authorities** provide guidelines and case studies on all lawful grounds, including consent for processing personal data for different purposes: **European Union:** European Data Protection Board Guidelines **United Kingdom:** Information Commissioner's Office Guidance on sharing personal information for mitigating scams and fraud

Rights

PRINCIPLE | A smart data privacy law is one that includes a range of rights to empower individuals.

Rights can help individuals understand what data an organisation holds about them and to exert a reasonable level of influence over the use of that data. Smart data privacy laws provide individuals or 'data subjects' the right to seek redress if their rights are not respected. Such rights include the right to access, correct, delete their data and object to processing.

In the mobile context, MNOs typically implement these rights through personal data management platforms and tools managed by data privacy or compliance teams responsible for individual rights, and creative data subject rights campaigns and awareness.

Lack of resources, budget, time, platforms and management tools are the key challenges for organisations in fulfilling a data subject's rights. Established supervisory authorities operating in advanced jurisdictions have acknowledged the amount of time and costs associated with complex multijurisdictional data subject access, data deletion and data portability requests.

> "Communicating individual or data subject rights require contextual sensitivity to a country's culture, people, customs, and traditions. Simplicity and relatability should be the way forward."
>
> MNO insight at the MWC 2025 Barcelona Ministerial Programme.

For a successful and smart implementation outcome, it is important that supervisory authorities:

- **Minimise prescriptive requirements** and explain how reducing documentation formality and process can lead to improved effectiveness and efficiency.
- **Support innovation** by encouraging organisations to consider automated platforms and tools as well as creative tools.

Smart Implementation	Examples
Outline practical, context-specific scenarios	**Use thematic websites** to help minimise formality and overly detailed requirements and improve efficiency of understanding of how user rights can be fulfilled: **Hong Kong:** Office of the Privacy Commissioner for Personal Data, Hong Kong website **Use creative communications techniques** to explain data rights to individuals in local languages: **Kenya:** Office of the Data Protection Commissioner Kenya, Personal Data Protection Handbook

Data breach notification

PRINCIPLE | A smart data privacy law is one that has a pragmatic approach to **data breach notifications.**

A smart data privacy law will express the time limit for reporting data breaches as a general standard, such as 'promptly' or 'without undue delay', rather than a specified number of hours and will set a threshold for reporting data breaches to individuals based on a high risk of harm to the affected individuals.

In the mobile context, MNOs are often subject to strict notification timelines (24-72 hours) as well as additional or different data breach notification requirements from telecoms sector specific or cybersecurity laws that overlap with the general data privacy law. This can be counterproductive (i.e., lead to higher risk for users of the affected MNO) and lead to over-notification to individuals resulting in confusion, fatigue and undermining trust.

> "Supervisory authorities should align and explore an integrated data breach notification model at local, regional and global level."
>
> Reflection of a former chief privacy officer of an MNO at the GSMA Ministerial Programme at MWC Barcelona 2025.

For a successful smart implementation outcome, it is important that supervisory authorities embrace the following principles:

- **Accountability:** Be clear to organisations on their obligations and whether they require notification with clear next steps and if the breach is likely to cause distress and harm to individuals.
- **Sensibility:** Collaborate with organisations, relevant sectoral supervisory authorities to understand the context and overlaps. Undertake periodic data breach and security reviews, generate learnings and improve the data breach notification model and implementation guidance.
- **Transparency:** Keep organisations informed on the outcome of investigations and assessments based on data security breach requirements.

Smart Implementation	Examples
Provide clear guidance and reviews	**France:** Commission Nationale de l'Informatique et des Libertés, France, provides a practical guide, including checklists and scenarios www.cnil.fr **Singapore:** The Personal Data Protection Commission, Singapore, outlines a data breach response tailored to the individual circumstances of the incident using the acronym C.A.R.E: Contain, Assess, Report, Evaluate. www.pdpc.gov.sg/ **Nigeria:** Nigeria Data Protection Commission resources ndpc.gov.ng/resources/

Cross-border data flows

PRINCIPLE | A smart data privacy law is one that promotes **cross-border data** flows.

The global digital economy depends on cross-border flows of data to deliver crucial social and economic benefits to individuals, businesses and governments. While the free flow of data across borders is essential, many jurisdictions place restrictions on the movement of data globally. Some of these restrictions may be unnecessary and can stifle innovation, efficiency and economic activity. The strategic role of cross-border data flows has been recognised by policymakers such as the OECD, the European Commission, UNCTAD and the ICC.

In the mobile context, the industry believes that cross-border data flows can be managed in ways that safeguard the personal data and privacy of individuals and is committed to working with stakeholders to ensure that restrictions are only implemented if they are necessary to achieve a legitimate public policy objective.

Regional data privacy initiatives such as the APEC Privacy Framework and Cross Border Privacy Rules (CBPR) and the EU's Binding Corporate Rules (BCR) have already moved in this direction, allowing organisations to transfer personal data generally under certain conditions. These regional frameworks are based on internationally accepted data protection principles, and on ensuring that the organisation transferring the data remains accountable for the subsequent use of the data. However, more needs to be done to make these frameworks easier to use, to encourage other regions to adopt similar frameworks and to make the frameworks interoperable.

For a successful smart implementation, it is important that supervisory authorities:

- Support frameworks for the movement of data and work to make these frameworks interoperable.
- Simplify and streamline cross-border data flow mechanisms and minimise overly prescriptive whitelist requirements.
- Consider alternative approaches to data localisation requirements, such as developing digital data embassies and data spaces.
- Support and promote industry best practices.

Smart Implementation

Simplify and streamline, avoiding overly prescriptive requirements while supporting interoperable mechanisms

Examples

EU and China launch cross-border data flow communication mechanism: policy.trade.ec.europa.eu

Association of Southeast Asian Nations: Joint guide to ASEAN MCCs and RIPD MCCs: https://asean.org/wp-content/uploads/2025/01/Joint-Guide-to-ASEAN-MCCs-and-RIPD-MCCs.pdf

UK: The ICO's comprehensive cross-border data flows guidance outlining requirements and mechanisms: ico.org.uk/for-organisations

EU: The European Commission's guide on cross-border data flows to adequate third countries (also known as whitelist): commission.europa.eu

Association of Southeast Asian Nations: The ASEAN regional model standard contractual clauses that can be incorporated in contracts, data transfer and sharing agreements: asean.org

The Global Cross-Border Privacy Rules (CBPR): The Global CBPR and the Global privacy Recognition for Processors (PRP) Systems: www.globalcbpr.org

Remedies, enforcement and sanctions

PRINCIPLE | A smart data privacy law is one that provides a range of remedies, enforcement measures and sanctions that are proportionate to the harm and take an organisation's good practices into account.

Remedies, enforcement measures and sanctions are necessary to give genuine and proportionate redress for individuals who have suffered significant harm.

In the mobile context, MNOs are often subject to additional or different telecommunications sector-specific or cybersecurity laws that overlap with general data privacy laws. As data protection supervisory authorities tend to implement the law through enforcement guidance, the provisions of the data privacy enforcement guidance may overlap with telecoms or other regulatory guidance or approach.

For a successful smart implementation, it is important that supervisory authorities:

- Work collaboratively with the relevant other regulators to ensure a consistent and co-ordinated response.
- Collaborate on the scope of enforcement, stay regularly in contact and share updates on the progress of investigations and findings.
- Identify and streamline priority enforcement topics, including fact-finding exercises and lessons learned from previous investigations.
- Identify types of organisations and stakeholders to reach out to as part of coordinated enforcement based on strategy, enforcement priorities, resources and agreed scope.

Smart Implementation	Examples
Develop an efficient and coordinated enforcement framework	**Coordination frameworks on both a national and international basis:** **Asia Pacific Privacy Authorities (APPA)** activities and privacy awareness week www.appaforum.org/news/ www.appaforum.org/paw/ **Ibero-American Data Protection Network (RIPD)** activities www.redipd.org/en/activities **UK:** The United Kingdom's Digital Regulation Cooperation Forum (DCRF) brings together the Information Commissioner's Office (ICO), the Competition and Markets Authority (CMA), the Office of Communications (Ofcom) and the Financial Conduct Authority (FCA). It was established to ensure a greater level of cooperation given the unique challenges posed by regulation of online platforms and digital services. www.drcf.org.uk **The Global Privacy Enforcement Network (GPEN)** is an informal network of privacy enforcement authorities focused on cross-border cooperation in enforcing privacy laws. It facilitates cooperation among privacy regulators worldwide to strengthen personal privacy protections in an increasingly globalised world. GPEN conducts annual "sweeps" to assess global privacy practices and identify areas for improvement. www.privacyenforcement.net/content/home-public **Network of African Data Protection Authorities (NADPA-RAPDP)** Annual General Meeting www.rapdp.org/en/qui-sommes-nous

Conclusion

Achieving the right outcomes for the digital age requires a smart approach to regulation, as well as a trusted mobile ecosystem. Smart implementation is not about rigid enforcement or overly prescriptive requirements, but about creating a flexible, transparent and inclusive framework that enables the digital economy whilst safeguarding the personal data and privacy of individuals.

The role of supervisory authorities in shaping the future of connectivity is critical. As they continue to refine their approaches, collaboration, consultation and continuous learning will be vital to achieving meaningful and sustainable outcomes.

The GSMA is committed to collaborating with governments and policymakers on implementing the core principles of a smart data privacy law in order to foster innovation and empower individuals. We hope this report can both help inspire practical, risk-based, evidence-based and collaborative approaches. Governments and policymakers that need support are welcome to reach out to: policyandreg@gsma.com

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom
gsma.com